(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 August 2002 (22.08.2002)

PCT

(10) International Publication Number
WO 02/065696 A1

(51) International Patent Classification[7]: H04L 9/32, G06K 19/10, G06F 1/00

(21) International Application Number: PCT/SE02/00243

(22) International Filing Date: 13 February 2002 (13.02.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0100474-6 14 February 2001 (14.02.2001) SE

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HANSSON, Elisabeth** [SE/SE]; Tallholmsvägen 169, S-589 37 Linköping (SE). **PERSSON, Håkan** [SE/SE]; Violabergsvägen 4, S-136 68 Haninge (SE).

(74) Agents: **NILSSON, Ellen** et al.; Albihns Stockholm AB, P.O. Box 5581, S-114 85 Stockholm (SE).

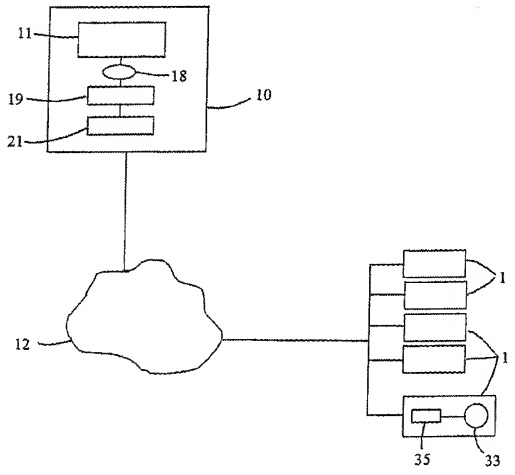
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A SECURITY ARCHITECTURE



(57) Abstract: A method for distributing private keys and certificates to cryptographic devices (1). According to the invention the method comprises the steps of: providing a first CA-system (5) at the manufacture of the devices; providing a temporary private key and a temporary certificate from the first CA-system (5) to each device (1) during the manufacturing of the device (1); delivering said devices (1) to customers; providing a second CA-system (11) at a customer node (10), this being performed at this process step or earlier in the process; for each delivered cryptographic device: connecting the device to a network, which is reachable from the customer node (10); authenticating the device as being from said manufacture; automatically replacing the temporary private key and the temporary certificate with a new private key and a new certificate and also automatically providing the device with a CA-certificate, the new certificates being signed by the second CA-system (11) which is notified of the connection of the device (1) as soon as the device (1) has connected to the network.

WO 02/065696 A1

A security architecture

TECHNICAL FIELD OF THE INVENTION

The present invention relates to a method for distributing private keys and certificates to cryptographic devices.

It also relates to a system used to distribute private keys and certificates to cryptographic devices.

Furthermore it relates to a cryptographic device.

RELATED ART

Data traffic over insecure networks, such as Internet, is an area where encryption and authentication become more and more common. In many devices it is critical to know whom one is communicating with and it is also critical to know that information received not has been changed by someone who is unauthorised. Examples of such devices are an e-box, a BSC (Base Station Controller) or any device which is connected to an insecure network and is being used for electronic commerce, bank services, control, supervision etc. These devices need security mechanisms such as authentication, integrity and maybe confidentiality.

For a security solution to work the usage of asymmetric keys are required. The sender of an authenticated message uses its private key to provide authenticity of the message and the receiver applies the sender's public key to verify the message.

The way the private and public keys are distributed and used is called a Public Key Infrastructure (PKI). The present invention discloses a method to distribute the keys in an effective and secure way.

A private key and its corresponding public key (a key pair) can either be generated by the device itself or by a central body and then be distributed to the device.

For a certain security solution to work, a certain public key must be connected to the correct identity. If central distribution of keys is used the device's public key is stored in a directory. Every time an authentication is performed or when a confidential message is to be sent, the correct public key is retrieved from the directory. The main problems with this method are the administrative issues regarding populating the directory and keeping the integrity of the information stored. A common solution to this is to generate X.509 certificates, where a public key and its corresponding identity is stored in an electronic document and then digitally signed by an Certification Authority (CA). The signature will prevent the manipulation of the information in the certificate.

Since the X.509 certificate does not include any secret information, it can be transmitted together with e.g. a signed message or during the handshake phase of SSL-(Secure Socket Layer)-communication. This will make all the PKI-based security solutions easy to handle.

A certificate is verified in the same way as a normal signed document. All units having access to the issuer's public key are able to verify the certificate. The issuer is the CA-system, which has signed the certificate. The issuer's public key is also included in a certificate called root-certificate or CA-certificate.

Authentication is a security mechanism in which a stated identity (or role) is proven. There are mainly two types of authentication; weak and strong authentication. The two types differ in the way the identity is proven. The commonly used way in weak authentication is that a static password (or similar) is connected to an identity and input when the authentication is required. The commonly used way in strong authentication is that the password connected to the identity is "random" (from an intruder's point of view) and the same password is never entered or sent twice. The "random" password is

often the result of a symmetric or asymmetric encryption, with the latter being the most common in new solutions. To be able to perform two-way strong authentication the server side and client side need to possess a private key, certificate and CA-certificate.

To be able to perform server strong authentication, the server side must possess a private key and a certificate. When the client generates a challenge, which is sent to the server, the server encrypts the challenge with the server's private key. The encrypted challenge is sent back to the client together with the server certificate. The client verifies the received certificate using the CA-certificate. The answer is decrypted with the servers public key included in the certificate and if the decrypted answer equals the sent challenge the connection is accepted. Client authentication is performed in the same way but this time the client needs a private key and a certificate and the CA-certificate has to be present in the server.

Authentication is not limited to physical users but can also be performed between two machines or applications.

Here below some important words relating to security will be described:

i) Authorization or access control is the mechanism in which an access to a certain resource is granted or not.

ii) Integrity of the data passed is often essential to two communicating parties. This means that a receiver of the data wants to be certain that the data received is consistent with the data that was sent.

iii) Confidentiality protects against disclosure to unauthorised identities.

iv) The Non-repudiation security service prevents that someone falsely denies that a transaction or a communication has occurred. This is often called digital signature since the Non-repudiation service can be used to generate a digital correspondence to a

normal non-digital and signed document. Non-repudiation is a combination of authentication and integrity, i.e. the identity of the sender of the data is established and the data received is consistent with the data sent.

v) Signing/verification comprises authentication, integrity and the feature that the sender not is able to deny a sent message. The sender is signing the message and the receiver is verifying the message.

Much of the security in the described security services depends on the user or device control of the private key used in the services. If a private key used in, e.g., an authentication procedure is not under control of the user or device that is subject to the authentication, the authentication can easily be forged. This is the same for all security services.

Http (Hyper-Text Transfer Protocol) can use SSL to secure all traffic that is passed through a certain TCP(Transmission Control Protocol) socket. This is called https (Hyper-Text Transfer Protocol, Secure variant). When the SSL-connection is established and data is passed over to the server application a handshake phase is executed. In this phase encryption keys are exchanged and authentication is performed.

The private keys and certificates could be saved in a number of different ways. Hard smart cards and soft smart cards, i.e. a software file, are the two most common ways. A hard smart card is a tamper resistant device on which the key and certificate are stored. The device executes the algorithm internally. With this method, the private key will never leave its protected storage. The key is protected on the smart card and it can be distributed in an arbitrary way to the customer. Using a soft smart card means that the private key is stored in an ordinary software file, e.g. PKCS12-file, PEM-file etc. However an entity's private key must be protected from disclosure and unauthorised usage and this is most commonly accomplished by encrypting the private key using a password (a pass-phrase) as the encryption/decryption key.

It is important that the private key is protected from disclosure during manufacturing, distribution and when the private key is loaded in the device. The private key must also be protected from disclosure inside the device. Another problem related to private keys and certificates is customization. Customization means the procedure to connect a device to a specific customer. Normally, the device is customized at the time when the device gets its private key.

Solutions using hard smart cards suffer from the drawback that these solutions end up to be very expensive. The card itself may not be very expensive but you need also to have a reader for the hard smart card and software to be able to read from the card etc. There are different solutions using soft smart cards present today. One problem with these solutions is the lack of security. One today common way to store the files and distribute them is to store them on a floppy disk and then insert the disks in the devices. This method is not as secure as desirable and the method is also rather costly. Someone unauthorised could get hold of a disk and the manually inserting of the disk into the device is expensive.

SUMMARY

One object of the present invention is to provide a security architecture that solves the distribution and customization problems in a new way that is less expensive than the known solutions.

It is also an object of the invention to provide a security architecture that solves the distribution and customization problems in a new way that is effective, secure and automatic.

These objects are achieved in a method as described initially that comprises the steps of:

- providing a first CA-system at the manufacture of the devices;

- providing a temporary private key and a temporary certificate from the first CA-system to each device during the manufacturing of the device;
- delivering said devices to customers;
- providing a second CA-system at a customer node, this being performed at this process step or earlier in the process;

for each delivered cryptographic device:

- connecting the device to a network, which is reachable from the customer node;
- authenticating the device as being from said manufacture;
- automatically replacing the temporary private key and the temporary certificate with a new private key and a new certificate and also automatically providing the device with a CA-certificate, the new certificates being signed by the second CA-system which is notified of the connection of the device as soon as the device has connected to the network.

The objects are also achieved by a system as initially described, which comprises:

- a first CA-system located at the manufacture of the devices, which first CA-system is adapted to provide the device with a temporary private key and a temporary certificate during the manufacture of the device;
- a second CA-system, being the customer's CA-system, located in a customer node, which is reachable from the device when it has been connected to a network by, for example the end user, said second CA-system being adapted to provide the device with a new private key, a new certificate which is signed by the second CA-system and with a CA-certificate, said new private key and new certificate being adapted to automatically replace the temporary private key and the temporary certificate in the device when the device is being customized;
- an authentication module being adapted to verify that the device has been produced at said manufacture by using a factory CA-certificate provided to the authentication module from the first CA-system.

The objects are also achieved in a cryptographic device, which is adapted to receive a temporary private key and a temporary certificate from a first CA-system provided at

the site of manufacture during the manufacture of the device. Furthermore the device comprises an activating client, which is adapted to be activated as soon as the device is connected to a network and an address to a customer node has been provided. The activating client is adapted to replace the temporary private key and the temporary certificate with a new private key, a new certificate and a CA-certificate, the certificates being signed by a second CA-system comprised in the customer node, which is reachable from the network.

When this method, system and device are used, the distribution of private keys and certificates to cryptographic devices and the customization of the devices are performed automatically.

Preferably the method further comprises the steps of:

- loading software, for example a first CA-client, which is adapted to send out a request for the temporary private key and the temporary certificate to the first CA-system, in the device by using a loading station provided at the site of manufacture during the manufacture;
- indicating to the device from the loading station that it is time to request a temporary private key and a temporary certificate from the fist CA-system;
- sending the request from the device to the first CA-system as an xml-(extensible mark-up language)-request;
- storing the retrieved temporary private key and temporary certificate in the device.

Hereby the distribution of a temporary private key and a temporary certificate during the manufacture of the device is performed automatically.

Advantageously the method further comprises the steps of:

- automatically sending out a request for a new private key, a new certificate and a CA-certificate from the device to the customer node as soon as the device has been connected to the network and the address to the customer node has been provided;

- authenticating the device in an authentication module comprised in the customer node by using a factory CA-certificate provided to the authentication module from the first CA-system;
- if the authentication was successful, forwarding the request to an authorization module connected to the authentication module, to verify if the request should be allowed and the device should be provided with new keys and certificates from the second CA-system;
- if the authorization was successful, forwarding the request to a second CA-client, which forwards the request as an xml-request to the second CA-system, which is connected to the second CA-client;
- answering with a new private key, a new signed certificate and also with a CA-certificate from the second CA-system;
- forwarding the answer to the requesting device;
- replacing the temporary private key and the temporary certificate with the new private key and the new certificate and storing them together with the CA-certificate in the device.

Hereby the distribution of a new private key, a new certificate and a CA-certificate is performed automatically. Also the customization of the device is performed automatically. The distribution is also secure.

Alternatively the method further comprises the steps of:

- providing the device with a CA-certificate from the first CA-system during the manufacture;
- automatically sending out a request for a new private key, a new certificate and a CA-certificate from the device to the customer node as soon as the device has been connected to the network and the address to the customer node has been provided;
- authenticating the device in an authentication module comprised in the customer node by using a factory CA-certificate provided to the authentication module from the first CA-system;

- authenticating the customer node in the device by using the CA-certificate provided to the device during the manufacture;
- if the authentication in the customer node and the device was successful, forwarding the request to an authorization module comprised in the customer node to verify if the request should be allowed and the device should be provided with new keys and certificates from the second CA-system;
- if the authorization was successful, forwarding the request to a second CA-client, which forwards the request as an xml-request to the second CA-system, which is connected to the second CA-client;
- answering with a new private key, a new signed certificate and also with a CA-certificate from the second CA-system;
- forwarding the answer to the requesting device;
- replacing the temporary private key and the temporary certificate with the new private key and the new certificate and storing them together with the CA-certificate in the device.

Hereby a two way authentication is performed.

Preferably the method further comprises the steps of:

- sending the request from the device through a communication means provided in the device;
- signing the request in the communication means using the temporary private key before it is sent to the customer node;
- encrypting the request by the communication means before it is sent to the customer node;
- receiving and decrypting the answers from the second CA-system in the communication means.

Suitably the method comprises decrypting the request in an authentication module when the request from the device is received in the customer node and encrypting the answer in the authentication module before it is sent to the device.

Furthermore the method suitably comprises including the identity of the device and optional parameters in the request, this identity and the parameters being used in the configuration of the certificate.

Preferably the method further comprises the steps of:

- receiving a request for a new private key, a new certificate and a CA-certificate from the device in the second CA-system;
- generating a new private key, a new public key and configuring a new certificate comprising said new public key in the second CA-system;
- signing said new certificate and a CA-certificate in the second CA-system;
- automatically answering the request by sending the requested new private key, new certificate and CA-certificate to the device from the second CA-system.

Hereby the process in the second CA-system also is performed automatically.

Suitably the communication means is a https-proxy and the authentication module is a https-server. Hereby https could be used as the communication protocol.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic view of the process for manufacturing devices according to the invention.

Fig. 2 is a schematic view of a network to which devices are connected.

Fig. 3 is a flowchart of one embodiment of a process according to the invention.

Fig. 4 is a schematic view of a CA(Certification Authority)-system according to the invention.

Fig. 5 is a schematic view of a device according to the invention.

DETAILED DESCRIPTION OF EMBODIMENTS

The present invention discloses a software solution to the security problem. The necessary private keys and the certificates are stored in one or several software files.

Fig. 1 is a schematic view of the process for manufacturing devices according to the invention. A number of devices 1 are shown. They comprise all a first CA(Certification Authority)-client 3. A CA-client is in this application defined to be means for automatically creating a request of a private key, a certificate and optionally a CA-certificate from a CA-system. The first CA-clients 3 are in contact with a first CA-system 5 provided at the site of manufacture here called a factory. The network between the devices and the first CA-system 5, in the factory is a "secure network". A "secure network" is here a private network to which no one that is unauthorised has access. The devices 1 are also connected to a loading station 4 through a "secure network". This loading station 4 has two important functions. The first is to load software, for example the first CA-client 3, to the devices 1 and the second is to inform the device 1 of when it is time to make the request for a private key and a certificate.

The devices are cryptographic devices. They include at least one private key and a certificate, which are used for signing/verification. A cryptographic device is a device, which comprises software for encrypting and decrypting and possibly also software for performing digital signing/verification. The device could for example be an e-box, a set-top-box, a BSC (Base Station Controller) or any device which needs private keys and certificates for signing/verification and/or encryption/decryption.

When the loading station 4 has informed the device 1 that it is time to make a request, the first CA-client 3 in the device 1 automatically requires a first temporary private key and a first temporary certificate and optionally a CA-certificate from the first CA-system 5. The request is sent over a TCP/IP and it includes the identity of the device

and some optionally parameters such as the length of the keys, the validity of the certificate, the name of the CA-server etc. These parameters are used in the configuration of the certificate. The keys are given the specified length and some of the other parameters are included in the certificate. If no optionally parameters are provided from the device the CA-system uses default values. The first CA-system 5 generates a private key and a public key. The public key is included in a certificate and the certificate is signed by the CA-system. The CA-system then transfers the key and the certificate to the first CA-client 3. Optionally a CA-certificate could also be provided to the device 1. The device 1 stores the key and certificate/s and comprises thus a first temporary private key and a first temporary signed certificate and optionally a CA-certificate when it leaves the factory. The devices are not tied to a specific customer when they leave the factory. The connection to a specific customer is established first when the temporary key and certificate are replaced by new ones provided from a customer CA-system. This is described further down in the description.

In an alternative embodiment the first CA-client 3 is positioned outside the devices 1 in the factory. This CA-client could then be used by more than one device 1 to request temporary keys and certificates during the manufacture.

Fig. 2 is a schematic view of a network given as an example to which the device 1 could be connected. The device 1 is connected to a customer node 10 via one or several networks 12 and optionally via one or several hosts (e.g.firewall). The networks could be insecure networks such as Internet.

The customer node 10 comprises a second CA-system 11 being the customer's own CA-system, a second CA-client 18 connected to the CA-system 11, an authorization module 19 connected to the second CA-client 18 and an authentication module 21 connected to the authorization module 19. The authentication module 21 could be a web-server. In one preferred embodiment it is an https-server. The customer is in this case not necessarily the owner of the device but rather the owner of the network or the one who manages the devices.

A number of devices 1 according to the invention are connected to the network. One of the devices 1 is shown to comprise an activating client 33 and a communication means 35. The communication means 35 should be able to crypt/decrypt and sign and possibly verify requests. The communication means 35 is in one embodiment an https-proxy. When, for example, an end user or an installation engineer connects the device 1 to the network and indicates the address to the customer node 10 the activating client 33 is activated and sends automatically out a request for a new private key, a new certificate and a CA-certificate. The temporary private key, which was provided to the device at the factory, is used to sign the request for a new private key, a new certificate and a CA-certificate. This is done in the communication means 35 when the request is sent from the device 1. A factory CA-certificate provided from the first CA-system in the factory to the authentication module 21 in the customer node 10 in the network is used to verify the request. The temporary private key and the temporary certificate are replaced by a new private key and a new certificate signed by the second CA-system 11. A CA-certificate is also provided to the device 1 from the second CA-system 11. When the device 1 has received and stored the new private key, certificate and CA-certificate the customization is completed and the device is tied to the specific customer, which provides the second CA-system 11. The retrieved new private key, certificate and CA-certificate are then used by the device 1 for secure connections.

Fig. 3 is a flowchart of one embodiment of a process according to the invention. The process will here below be described with reference to Figure 1, 2 and 3. The process starts with the manufacturing of one device 1. In block B41 the loading station 4 loads

ple of the type of request. The CA-system 5 generates a private and a public key, includes the public key in a certificate and signs the certificate in block B44 and in block B45 a reply with the private key and the certificate is sent to the first CA-client 3. In block B46 the temporary key and certificate are stored in the device 1.

The device 1 is then delivered to a customer and in block B47 the device 1 is connected to an insecure network by, e.g. an end user or an installation engineer. When the end user gives the name or address to the customer node 10 the activating client 33 is activated and a request for a new private key, certificate and a CA-certificate is sent out from the activating client 33. This is shown in block B49. It is not necessarily the end user who gives the address to the customer node 10. The address could for example be pushed out to the device 1 from another unit or the end user could give the address to another unit, which knows the address of the customer node 10. It is also possible that more input data is needed from the end user before the request for a new key and certificate is sent out. The request is in block B51 sent through the communication means 35 for ensuring a secure communication. The request is signed by the communication means 35 using the first temporary private key provided at the factory. The request is also encrypted by the communication means 35 before leaving the device 1. In block B53 the request is forwarded through the network/s to the customer node 10. In block B55 the request is received in the authentication module 21, which in this embodiment is a web-server and in block B57 the web-server 21 uses strong authentication to authenticate the device, i.e. verify that the device 1 is produced at the factory. The factory CA-certificate has been distributed to the web-server 21 from the factory and is used for the authentication. The authentication module 21 also decrypts the request. If two way authentication is used the authentication module 21 also signs an answer which is sent back to the device. The communication means 35 uses the CA-certificate that optionally was provided to the device 1 at the factory to authenticate the customer node.

If the one or optionally the two way authentication was successful the request is forwarded to the authorization module 19 in the customer node 10. This is done in block

B59 and in block B61 the authorization module 19 first retrieves the identity of the device from the temporary certificate and then uses this identity to verify that the device has the right to receive keys from this specific CA-server. The authorization module 19 uses thus an internal database including access control register, where all valid devices and their identities are listed. Furthermore the authorization module 19 verifies that keys have not been distributed to this device before. If the authorization was successful the authorization module 19 forwards the request in block B62 to the second CA-client 18, which forwards the request of a private key, a certificate and a CA-certificate as an xml-request to the second CA-system 11. This is shown in block B63. The connection is done over TCP/IP and it is xml-encoded. The identity of the device is included in the request. Other parameters such as the length of the keys, the validity period of the certificate, the name of the CA-server, the locality, if the private key should be encrypted or not, if a CA-certificate should be included in the answer, organisation, organisation unit, email etc. are also optionally included in the xml-request. These parameters and the identity of the device are used for the configuration of the certificate. In block B65 the second CA-system 11 generates a key, a certificate and a CA-certificate and in block B67 the second CA-system 11 signs the certificates. Thereafter, in block B69, a reply comprising a new private key, a new signed certificate and a signed CA-certificate is sent from the second CA-system 11 to the second CA-client 18 and in block B71 this key and certificates are forwarded through the customer node 10 and the communication means 35 to the activating client 33 in the device 1. The reply is encrypted in the authentication module 21 and it is decrypted in the communication means 35. Finally, in block B73, the device 1 stores the new private key, the new certificate and the CA-certificate and thus the old first temporary private key and the first temporary certificate are replaced.

If a CA-certificate was provided to the device during the manufacturing this CA-certificate is used to verify the respond from the customer node 10.

Fig. 4 is a schematic view of a CA-system according to one embodiment of the invention. It comprises a receiving means 81. The receiving means 81 is adapted to receive

requests for keys and certificates from the devices. The receiving means 81 should also be able to receive the parameters that are used for the configuration of the certificate as described above. The receiving means 81 should comprise software to receive the request over TCP/IP and also software to understand an xml-request. The CA-system comprises also answering means 83 adapted to return private keys and signed certificates and possibly also CA-certificates over TCP/IP to the devices. The answer is xml-encoded. Furthermore it comprises generating means 85 adapted to generate private keys and public keys and certificates comprising said public keys together with certain parameters. The CA-system comprises furthermore signing means 87 adapted to sign certificates. The receiving of requests, the generating of keys and certificates and the replying to the requests, which replies comprise the generated keys and certificates, is done totally automatic. There is no manual treating of the CA-system after the configuration of the same. One first CA-system 5 is adapted to be located at the factory and a second CA-system 11 is adapted to be located in the customer network. This second CA-system 11 is adapted to return CA-certificates together with the private key and certificate to the requesting devices. The CA-system can comprise more than one CA, i.e. several CA:s where each CA has its own root-certificate and root-private-key.

Fig. 5 is a schematic view of a device 1 according to one embodiment of the invention. It comprises a first CA-client 3 adapted to during the manufacturing request the first temporary private key and the temporary certificate from the first CA-system 5 (Fig. 1) located at the factory. It comprises also a memory 93 in which the keys and certificates are stored. Furthermore it comprises an activating client 33, which is adapted to be activated as soon as the device has been connected to an insecure network by e.g. an end user and the address to the customer node 10 has been given. The activating client 33 is adapted to replace the temporary private key and the temporary certificate stored in the device 1 with a new private key, a new certificate signed by the second CA-system 11 (Fig. 2) connected to the network and a CA-certificate. In one embodiment the activating client 33 sends out a request through a communication means 35 for a new private key, a new certificate and a CA-certificate. The request is sent to the second CA-system 11. The communication means 35 ensures that the communication out from the

device is secure. It signs and encrypts the request. It also performs decryption of the retrieved answers.

The device 1 can store the private key and the certificate and optionally the CA-certificate encrypted in the memory 93.

It has been described that the second CA-system generates the new private key and the new certificate. This is not necessary. The private key and the certificate could be generated in another unit, which can reach both the device and the CA-system. A further possible variant is that the device itself generates the private and the public key. These two variants are possible as long as the new certificate is signed by the second CA-system.

In another embodiment of the invention a hierarchy of CA-systems could be present instead of the single second CA-system. In this case another CA-system (e.g. verisign) will sign the factory CA-certificate and optionally the customer CA-certificate. The device, the authentication module or any module can use a CA-certificate from the other CA to perform verification.

The here-described security architecture also makes it possible to protect the private key from disclosure in an efficient way. One alternative is to construct the device in a way that the device always requires strong authentication. Another alternative is to put the private key and certificate in a tamper device inside the device. The private key will never leave its protected storage inside the device (like a hard smart card). Both alternatives provide high security. Furthermore this solution provides a high security during the distribution of the keys, since the distribution is done automatically and nothing is done manually.

CLAIMS

1. A method for distributing private keys and certificates to cryptographic devices (1), **characterised in that** it comprises the steps of:
   - providing a first CA-system (5) at the manufacture of the devices;
   - providing a temporary private key and a temporary certificate from the first CA-system (5) to each device (1) during the manufacture of the device (1);
   - delivering said devices (1) to customers;
   - providing a second CA-system (11) at a customer node (10), this being performed at this process step or earlier in the process;

   for each delivered cryptographic device:
   - connecting the device (1) to a network, which is reachable from the customer node (10);
   - authenticating the device (1) as being from said manufacture;
   - automatically replacing the temporary private key and the temporary certificate with a new private key and a new certificate and also automatically providing the device with a CA-certificate, the new certificates being signed by the second CA-system (11) which is notified of the connection of the device (1) as soon as the device (1) has connected to the network.

2. A method according to claim 1, **characterised in that** it further comprises the steps of:
   - loading software, for example a first CA-client, which is adapted to send out a request for the temporary private key and the temporary certificate to the first CA-system (5), in the device (1) by using a loading station (4) provided at the site of manufacture during the manufacture;
   - indicating to the device (1) from the loading station (4) that it is time to request a temporary private key and a temporary certificate from the first CA-system (5);
   - sending the request from the device (1) to the first CA-system as an xml-(extensible mark-up language)-request;

- storing the retrieved temporary private key and temporary certificate in the device (1).

3. A method according to claim 1 or 2, **characterised in that** it further comprises the steps of:
- automatically sending out a request for a new private key, a new certificate and a CA-certificate from the device to the customer node (10) as soon as the device (1) has been connected to the network and the address to the customer node (10) has been provided;
- authenticating the device in an authentication module (21) comprised in the customer node (10) by using a factory CA-certificate provided to the authentication module (21) from the first CA-system;
- if the authentication was successful, forwarding the request to an authorization module (19) connected to the authentication module (21), to verify if the request should be allowed and the device (1) should be provided with new keys and certificates from the second CA-system (11);
- if the authorization was successful, forwarding the request to a second CA-client (18), which forwards the request as an xml-request to the second CA-system (11), which is connected to the second CA-client (18);
- answering with a new private key, a new signed certificate and also with a CA-certificate from the second CA-system (11);
- forwarding the answer to the requesting device (1);
- replacing the temporary private key and the temporary certificate with the new private key and the new certificate and storing them together with the CA-certificate in the device (1).

4. A method according to claim 1 or 2, characterised in that it further comprises the steps of:
- providing the device (1) with a CA-certificate from the first CA-system (5) during the manufacture;

- automatically sending out a request for a new private key, a new certificate and a CA-certificate from the device to the customer node (10) as soon as the device (1) has been connected to the network and the address to the customer node (10) has been provided;
- authenticating the device in an authentication module (21) comprised in the customer node (10) by using a factory CA-certificate provided to the authentication module (21) from the first CA-system;
- authenticating the customer node (11) in the device (1) by using the CA-certificate provided to the device (1) during the manufacture;
- if the authentication in the customer node (11) and the device (1) was successful, forwarding the request to an authorization module (19) comprised in the customer node (10) to verify if the request should be allowed and the device (1) should be provided with new keys and certificates from the second CA-system (11);
- if the authorization was successful, forwarding the request to a second CA-client (18), which forwards the request as an xml-request to the second CA-system (11), which is connected to the second CA-client (18);
- answering with a new private key, a new signed certificate and also with a CA-certificate from the second CA-system (11);
- forwarding the answer to the requesting device (1);
- replacing the temporary private key and the temporary certificate with the new private key and the new certificate and storing them together with the CA-certificate in the device (1).

5. A method according to any one of the claims 1-4, **characterised in that** it further comprises the steps of:
- sending the request from the device through a communication means (35) provided in the device;
- signing the request in the communication means (35) using the temporary private key before it is sent to the customer node (10);
- encrypting the request by the communication means (35) before it is sent to the customer node (10);

- receiving and decrypting the answers from the second CA-system (11) in the communication means (35).

6. A method according to any one of the preceding claims, **characterised in that** it comprises decrypting the request in an authentication module (21) when the request from the device (1) is received in the customer node (10) and encrypting the answer in the authentication module (21) before it is sent to the device (1).

7. A method according to any one of the claims 1-6, **characterised by** including the identity of the device and optional parameters in the request, this identity and the parameters being used in the configuration of the certificate.

8. A method according to any one of the preceding claims, **characterised in that** it further comprises the steps of:
- receiving a request for a new private key, a new certificate and a CA-certificate from the device (1) in the second CA-system (11);
- generating a new private key, a new public key and configuring a new certificate comprising said new public key in the second CA-system (11);
- signing said new certificate and a CA-certificate in the second CA-system (11);
- automatically answering the request by sending the requested new private key, new certificate and CA-certificate to the device (1) from the second CA-system.

9. A cryptographic device, **characterised in that** the device (1) is adapted to receive a temporary private key and a temporary certificate from a first CA-system (5) provided at the manufacture during the manufacture of the device (1) and in that it comprises an activating client (33) which is adapted to be activated as soon as the device is connected to a network and an address to a customer node (10) has been provided, the activating client (33) being adapted to replace the temporary private key and the temporary certificate with a new private key, a new certificate and a CA-certificate, the certificates being signed by a second CA-system (11) comprised in the customer node (10), which is reachable from the network.

10. A device according to claim 9, **characterised in that** the activating client (33) is adapted to send out a request for a new private key, a new certificate and a CA-certificate through a communication means (35), which is comprised in the device (1) and connected to the activating client (33), the request being sent to the customer node (10).

11. A device according to claim 10, **characterised in that** the communication means (35) is adapted to sign and encrypt the request before forwarding it to the customer node (10), the communication means (35) also being adapted to decrypt the received answers.

12. A device according to claim 11, **characterised in that** the communication means (35) is a https-proxy.

13. A device according to any one of the claims 9-12, **characterised in that** it comprises a first CA-client (3) adapted to request the first temporary private key and the temporary certificate from the first CA-system (5).

14. A system used to distribute private keys and certificates to cryptographic devices, **characterised in that** it comprises:

- a first CA-system (5) located at the manufacture, which first CA-system (5) is adapted to provide the device (1) with a temporary private key and a temporary certificate during the manufacture of the device (1);
- a second CA-system (11), being the customer's CA-system, located in a customer node (10), which is reachable from the device (1) when it has been connected to a network by, for example the end user, said second CA-system (11) being adapted to provide the device (1) with a new private key, a new certificate which is signed by the second CA-system and with a CA-certificate, said new private key and new certificate being adapted to automatically replace the temporary private key and the temporary certificate in the device (1) when the device (1) is being customized;

- an authentication module (21) being adapted to verify that the device (1) has been produced at said manufacture by using a factory CA-certificate provided to the authentication module (21) from the first CA-system (5).

15. A system according to claim 14, **characterised in that** the authentication module (21) is provided in the customer node (10) and is connected to the second CA-system (11) through an authorization module (19), which is adapted to verify if the request is allowed, and through a second CA-client, which is adapted to transform the request into an xml-request and forward it to the second CA-system (11).

16. A system according to claim 14 or 15, **characterised in that** the authentication module (21) is a https-server.

17. A system according to any one of the claims 14-16, **characterised in that** it comprises a communication means (35), which is located in the device (1) and is adapted to sign and encrypt the request before it is sent to the customer node (10) and decrypt and optionally verify the retrieved answer.

18. A system according to any one of the claims 14-17, **characterised in that** the system comprises a loading station (4) at the site of manufacture, which loading station (4) is adapted to load the necessary software, for example a first CA-client (3), which is adapted to send out a request for a temporary private key and a temporary certificate to the first CA-system (5), to the device (1) during the manufacture and also to indicate for the device (1) when it should send out the request to the first CA-system (5).

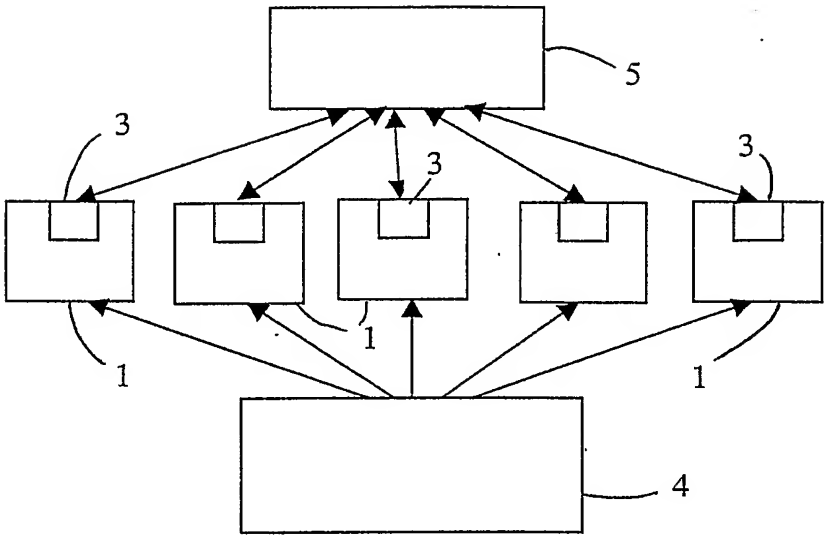


Fig.1

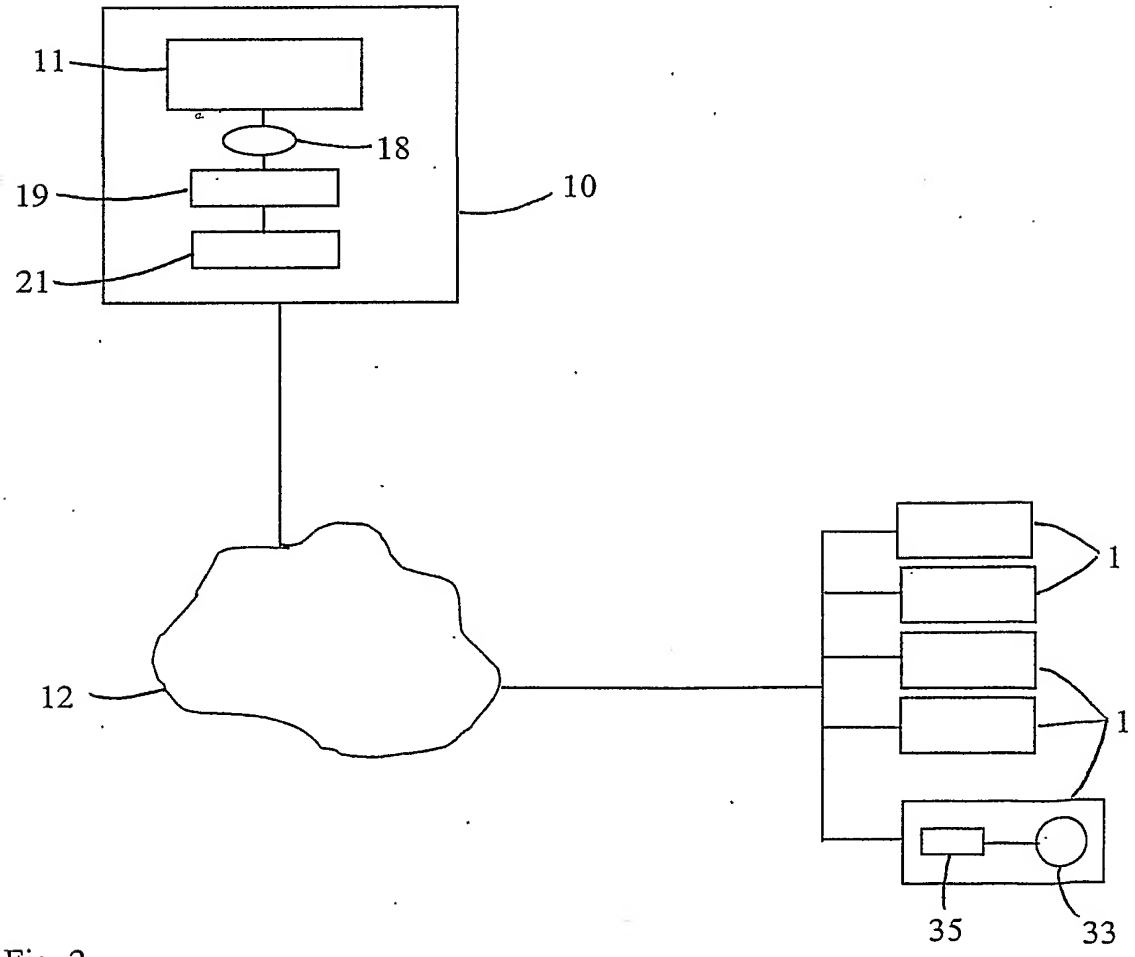


Fig. 2

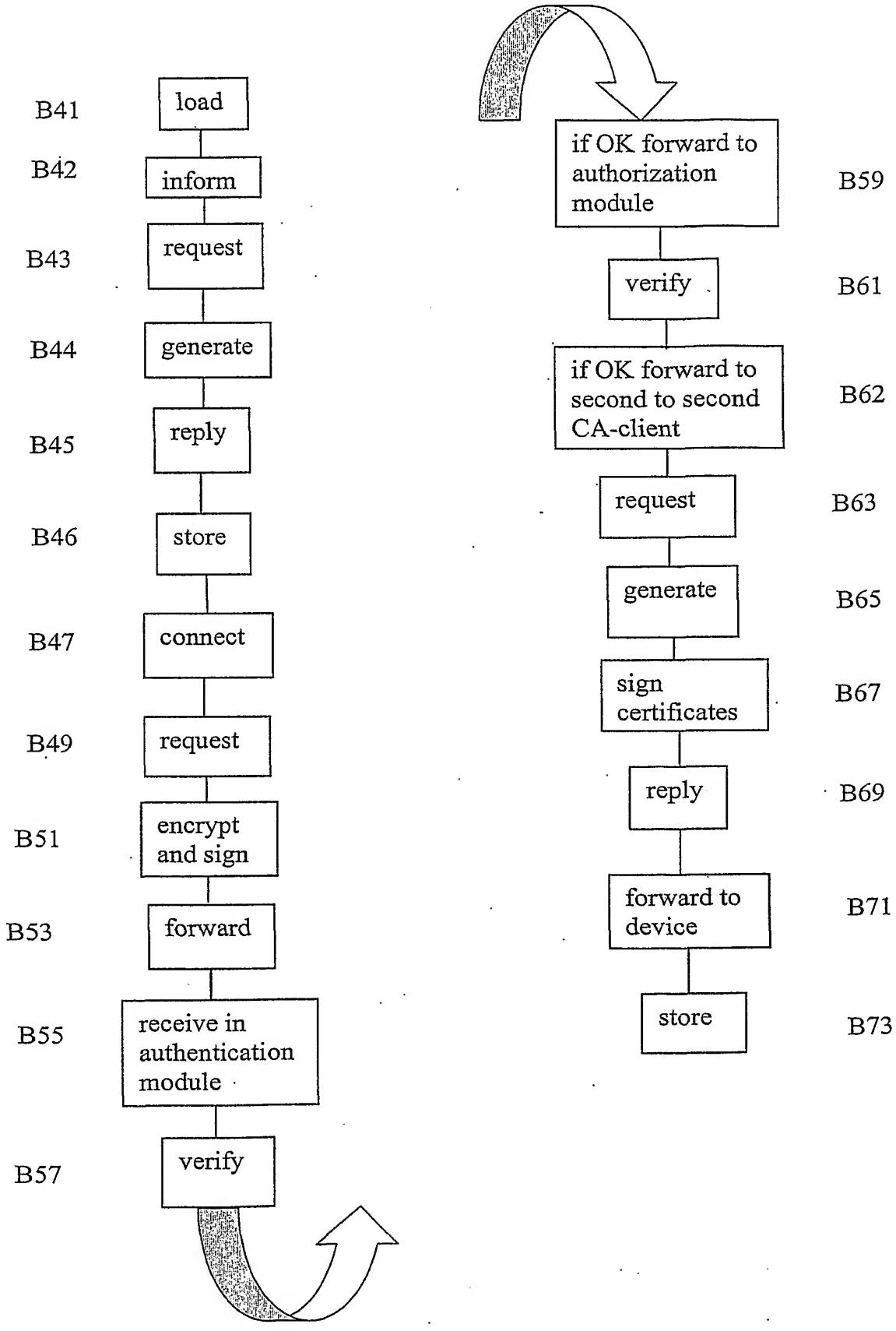

B41
load
B42
inform
B43
request
B44
generate
B45
reply
B46
store
B47
connect
B49
request
B51
encrypt and sign
B53
forward
B55
receive in authentication module
B57
verify
if OK forward to authorization module
B59
verify
B61
if OK forward to second to second CA-client
B62
request
B63
generate
B65
sign certificates
B67
reply
B69
forward to device
B71
store
B73

Fig.3

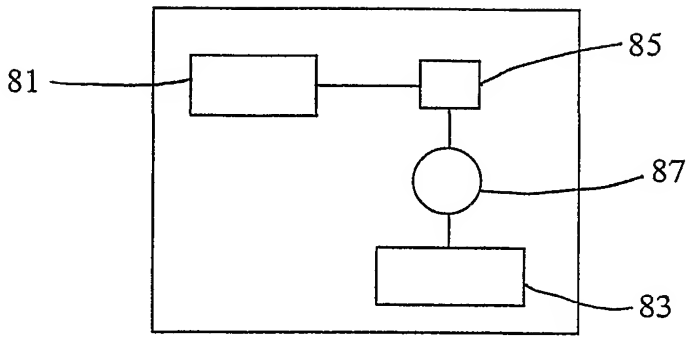


Fig.4

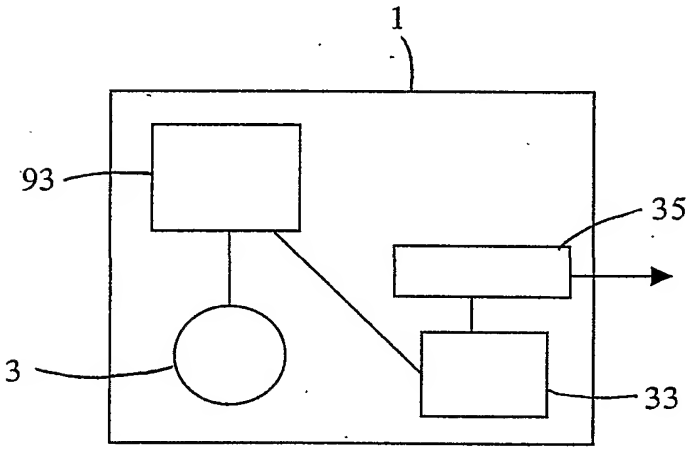


Fig.5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 02/00243

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/32, G06K 19/10, G06F 1/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, G06F, G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 0079724 A2 (NOKIA MOBILE PHONES LIMITED), 28 December 2000 (28.12.00), page 3, line 1 - page 4, line 27, claim 1, abstract --	1-18
Y	FERRARI, J. et al. "Smart Cards: A Case Study". IBM Redbooks [on line], October 1998 [retrieved on 2001-10-24] ISBN: 0738402931, Retrieved from the Internet: <URL: http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg245239.pdf>. Se page 87, paragraph 8 - page 88, paragraph 2; page 111, paragraph 2 - page 114, paragraph 6; chapter 12.4.1, figures 28, 42. --	1-18

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 April 2002	02 -05- 2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Pär Heimdal /OGU Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 02/00243

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6038551 A (BARLOW, D. ET AL), 14 March 2000 (14.03.00), column 2, line 63 - column 3, line 13, claims 9-10, abstract --.	1-18
A	US 5745574 A (MUFTIC, S.), 28 April 1998 (28.04.98), column 4, line 55 - column 8, line 14, figure 1, abstract --	1-18
A	WO 9957675 A1 (AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY), 11 November 1999 (11.11.99), page 3, line 9 - line 26, figure 1, claims 1,11, abstract --	1-18
A	WO 9935783 A1 (CYBERSAFE CORPORATION), 15 July 1999 (15.07.99), page 5, line 27 - page 7, line 6, abstract -- --------	1-18

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SE 02/00243

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0079724 A2	28/12/00	AU 5532800 A	09/01/01
		FR 2795262 A	22/12/00
		GB 0014816 D	00/00/00
		GB 2355151 A	11/04/01
		GB 9914262 D	00/00/00
US 6038551 A	14/03/00	NONE	
US 5745574 A	28/04/98	EP 1068697 A	17/01/01
		WO 9952242 A	14/10/99
WO 9957675 A1	11/11/99	AU 3784899 A	23/11/99
		BR 9910222 A	09/01/01
		CA 2330625 A	11/11/99
		CN 1308750 T	15/08/01
		EP 1076875 A	21/02/01
		US 6199762 B	13/03/01
WO 9935783 A1	15/07/99	AU 2452699 A	26/07/99
		CA 2313328 A	15/07/99
		DE 19918814 A	04/11/99
		EP 1042885 A	11/10/00
		JP 11334122 A	07/12/99
		JP 2002501218 T	15/01/02
		US 5949466 A	07/09/99
		AU 2392399 A	25/11/99
		BR 9901536 A	18/07/00
		CN 1235996 A	24/11/99
		EP 0960919 A	01/12/99
		JP 2000037656 A	08/02/00

PUB-NO: WO002065696A1
DOCUMENT-IDENTIFIER: WO 2065696 A1
TITLE: A SECURITY ARCHITECTURE
PUBN-DATE: August 22, 2002

INVENTOR-INFORMATION:

NAME	COUNTRY
HANSSON, ELISABETH	SE
PERSSON, HAAKAN	SE

ASSIGNEE-INFORMATION:

NAME	COUNTRY
ERICSSON TELEFON AB L M	SE
HANSSON ELISABETH	SE
PERSSON HAAKAN	SE

APPL-NO: SE00200243
APPL-DATE: February 13, 2002

PRIORITY-DATA: SE00100474A (February 14, 2001)

INT-CL (IPC): H04L009/32 , G06K019/10 , G06F001/00

EUR-CL (EPC): H04L009/32

ABSTRACT:

CHG DATE=20031129 STATUS=O>A method for distributing private keys and certificates to cryptographic devices (1). According to the

invention the method comprises the steps of: providing a first CA-system (5) at the manufacture of the devices; providing a temporary private key and a temporary certificate from the first CA-system (5) to each device (1) during the manufacturing of the device (1); delivering said devices (1) to customers; providing a second CA-system (11) at a customer node (10), this being performed at this process step or earlier in the process; for each delivered cryptographic device: connecting the device to a network, which is reachable from the customer node (10); authenticating the device as being from said manufacture; automatically replacing the temporary private key and the temporary certificate with a new private key and a new certificate and also automatically providing the device with a CA-certificate, the new certificates being signed by the second CA-system (11) which is notified of the connection of the device (1) as soon as the device (1) has connected to the network.